Notice of Allowability	Application No.	Applicant(s)	
	10/031,065	CORON ET AL.	
	Examiner	Art Unit	
	William S. Powers	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to _____.

2. ☒ The allowed claim(s) is/are *1-14*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 1/15/02
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060707* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Jacques Louis-Jacques
Supervisory Patent Examiner
Technology Center 2100

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with James LaBarre on July 7, 2006.

The application has been amended as follows:

Please amend Claims in accordance with Examiner's "Amendment to the Claims" included as pages 2-7 of this office action.

AMENDMENT TO THE CLAIMS

1. (Currently Amended) A method for performing cryptographic operations using keys obtained from random numbers that are generated using the Data Encryption Standard (DES) algorithm with a secret key K, said method taking as input a random integer s of size 64 bits, and an integer m, said method sending back as output m 64-bit random integers x_1, x_2, ..., x_m, said method comprising the following steps:

~~1~~a) ~~With~~with the DES algorithm and using the key K, ~~encrypt~~encrypting a value D representing date data and ~~put~~putting the result in an integer variable I;

~~2~~b) ~~For~~for j in the range 1 to m:

~~2a~~b1) ~~Replace~~replacing s by s XOR I,

~~2b~~2) ~~Define~~defining an integer variable y equal to the result of the encryption of s with the DES algorithm using the key K,

~~2c~~b3) ~~Put~~putting in x_j the result of y XOR s,

~~2d~~b4) ~~Replace~~replacing s with y XOR I,

~~2e~~b5) ~~Put~~putting in s the result of the encryption of s with the DES algorithm using the secret key K;

~~3~~c) ~~Return~~returning as output the succession (x_1, x_2, ..., x_m); ~~and~~

~~4) Performing cryptographic operations with~~d) obtaining keys corresponding to said values x_1, x_2, ...x_m; and

e) performing cryptographic operations with said keys.

2. (Currently Amended) A method for performing cryptographic operations using keys obtained from random numbers, said method taking as input a random integer s of size 64 bits and an integer m, and sending back as output m 64-bit random integers x_1, x_2, ..., x_m, by using the Data Encryption Standard (DES) with a secret key K, an integer intermediate variable y, and a source S of random integers ~~on~~of 64 bits ~~x_1, x_2, ..., x_m~~, said method comprising the following steps:

~~1~~a) ~~For~~for j in the range 1 to m:

~~1~~a1) ~~Generate~~generating an integer I by means of the source S,

~~1b) Replace s with s XOR I,~~

~~1c) Put in y the result of the encryption of s with the DES algorithm using the key K,~~

~~1d) Put in x_j the result of y XOR s,~~

~~1e) Replace s with y XOR I,~~

~~1f) Put in s the result of the encryption of s with the DES algorithm using the key K;~~

~~2) Return as output the succession (x_1, x_2, ..., x_m); and~~

a2) replacing s with s XOR I,

a3) putting in y the result of the encryption of s with the DES algorithm using the key K,

a4) putting in x_j the result of y XOR s,

a5) replacing s with y XOR I,

a6) putting in s the result of the encryption of s with the DES algorithm using the key K;

b) returning as output the succession (x_1, x_2, ..., x_m);

~~3) Performing cryptographic operations with~~ c) obtaining keys corresponding to said values x_1, x_2, ..., x_m~~.~~; and

d) performing cryptographic operations with said keys.

3. (Currently Amended) A handheld, wearable, or portable electronic device that executes the following steps to generate m 64-bit random integers x_1, x_2, ..., x_m:

~~1~~a) ~~With~~with the DES algorithm and using a key K, encrypt a value D representing date data and put the result in an integer variable I;

~~2~~b) ~~For~~for j in the range 1 to m:

~~2a~~b1) ~~Replace~~replacing a random integer s by s XOR I,

~~2~~b2) ~~Put~~putting in an integer variable y the result of the encryption of s with the DES algorithm using the key K,

~~2~~eb3) ~~Put~~putting in x_j the result of y XOR s,

~~2~~db4) ~~Replace~~replacing s with y XOR I,

~~2~~eb5) ~~Put~~putting in s the result of the encryption of s with the DES algorithm using the secret key K; ~~and~~

~~3~~c) ~~Return~~returning as output the succession $(x_1, x_2, ..., x_m)$~~.~~;

d) obtaining keys corresponding to said values $x_1, x_2, ..., x_m$; and

e) performing cryptographic operations with said keys.

4. (Previously Presented) An electronic device according to claim 3, wherein said device is a smart card.

5. (Previously Presented) An electronic device according to claim 3, wherein said device is a contactless card.

6. (Previously Presented) An electronic device according to claim 3, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

7. (Previously Presented) An electronic device according to claim 3, wherein said device is a badge.

8. (Previously Presented) An electronic device according to claim 3, wherein said device is a smart watch.

9. (Currently Amended) A handheld, wearable, or portable electronic device that executes the following steps to generate m 64-bit random integers $x_1, x_2, ..., x_m$:

~~1~~a) ~~For~~for j in the range l to m:

~~1~~a1) ~~Generate~~generating a 64-bit random integer I,

~~1b~~a2) ~~Replace~~replacing a 64-bit random integer s with s XOR I,

~~1c~~a3) ~~Put~~putting in an integer variable y the result of the encryption of s with the DES algorithm using the key ~~Y~~K,

~~1d~~a4) ~~Put~~putting in x_j the result of y XOR s,

~~1e~~a5) ~~Replace~~replacing s with y XOR I,

~~1f~~a6) ~~Put~~putting in s the result of the encryption of s with the DES algorithm using the key K; ~~and~~

~~2~~b) ~~Return~~returning as output the succession $(x_1, x_2, ..., x_m)$~~.~~;

c) obtaining keys corresponding to said values $x_1, x_2, ..., x_m$; and

d) performing cryptographic operations with said keys.

10. (Previously Presented) An electronic device according to claim 9, wherein said device is a smart card.

11. (Previously Presented) An electronic device according to claim 9, wherein said device is a contactless card.

12. (Previously Presented) An electronic device according to claim 9, wherein said device is a Personal Computer Memory Card International Association (PCMCIA) card.

13. (Previously Presented) An electronic device according to claim 9, wherein said device is a badge.

14. (Previously Presented) An electronic device according to claim 9, wherein said device is a smart watch.

AMENDMENTS TO THE SPECIFICATION

Page 4, following line 27 and immediately prior to the heading "**Description of the Invention**" inserted via the Preliminary Amendment filed January 15, 2002, add the following heading and new paragraphs:

Brief Description of the Drawings

Figure 1 is a flow chart of a first modified method of generating random numbers to make them capable of withstanding DPA-type attacks; and

Figure 2 is a flow chart of a second modified method of generating random numbers to make them capable of withstanding DPA-type attacks.

AMENDMENTS TO THE DRAWINGS

Please add the attached drawings, figures 1 and 2 to the application.

REASONS FOR ALLOWANCE

2. The following is an examiner's statement of reasons for allowance:

The present invention is directed to an improvement in a method for generating random numbers for use on smart cards as cryptographic keys. Each independent claim identifies the uniquely distinct feature of "putting in an integer

variable y the result of the encryption of s with the DES algorithm using the key K". The closest prior art, Applicant admitted ANSI Standard X9.17, does use the DES algorithm and XOR operations in the generation of a series of random numbers, but lacks the intermediate step cited above. With the additional DES encryption the claims recite an integer y to further randomize the generation of a series of random numbers that are then used as encryption keys. The aforementioned limitations are not in the prior art. In light of the foregoing, the claims of the present application are found to be allowable over the prior art of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to William S. Powers whose telephone number is 751 272 8573. The examiner can normally be reached on m-f 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on 571 272 6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

William S. Powers
Examiner
Art Unit 2134

7/13/2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

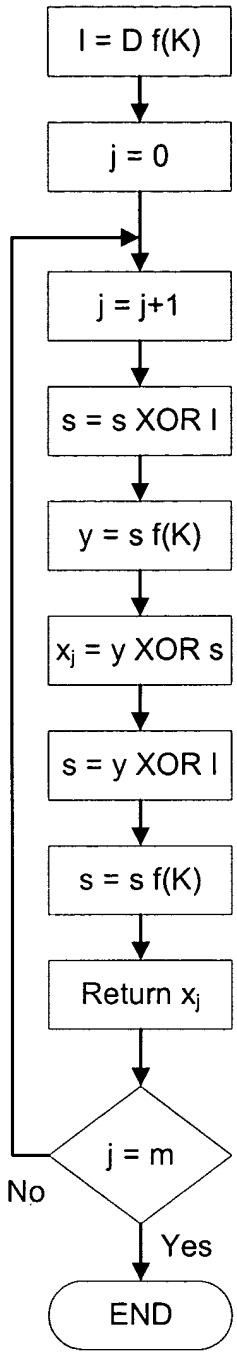
I = D f(K)
j = 0
j = j+1
s = s XOR I
y = s f(K)
x_j = y XOR s
s = y XOR I
s = s f(K)
Return x_j
j = m
No
Yes
END

Fig. 1

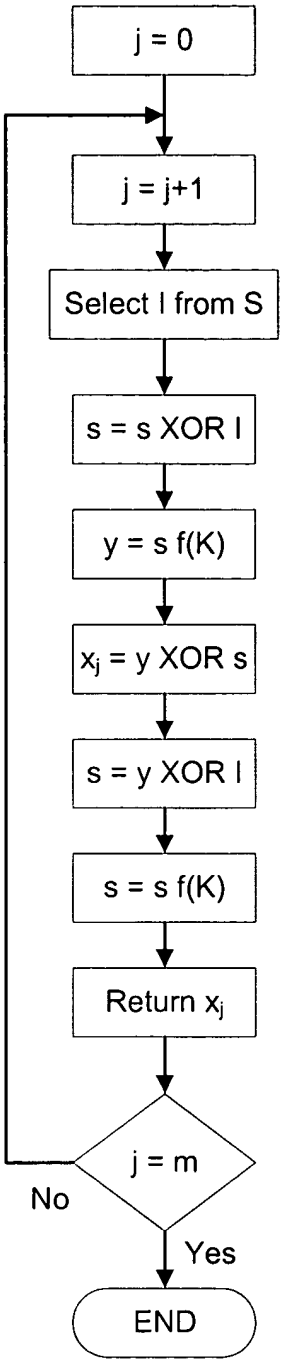
j = 0
j = j+1
Select I from S
s = s XOR I
y = s f(K)
x_j = y XOR s
s = y XOR I
s = s f(K)
Return x_j
j = m
No
Yes
END

Fig. 2